Commonwealth of Massachusetts
Executive Office for Administration and Finance
Information Technology Division

Policy Area: Enterprise Security	**Policy #:** ITD-SEC-5.1
Title: Enterprise Wireless Security Policy: Wireless Mobile Communications, Wireless Local Area Networks, Wireless Wide Area Networks, and Wireless Personal Area Networks	**Effective Date:** 08/24/06

Issue Statement

The proliferation of products for wireless communication, from WiFi Local Area Networks to mobile data, represents an important extension and complement to traditional wire-based networks. Wireless communication, however, also has significant limitations, including signal availability, reliability, data transmission rate and, most importantly, security vulnerabilities. Tools are readily available for an unauthorized, malicious user to capture data, crack passwords and tap sensitive or confidential information. State entities must adhere to the following standards-based policy to ensure the security, confidentiality, integrity, and availability of wireless communications.

Commonwealth agencies may use wireless technologies for a number of business purposes including LAN substitution and expansion, disaster recovery and emergency preparedness, emergency notification systems, system and data support for mobile workers, and applications for constituents and business partners that are optimized for wireless access. This policy addresses four major categories of wireless technology implementation:

Wireless Mobile Communications (WMC) utilize licensed frequencies and include such services as 2G and 3G cellular telecommunications, Cellular Digital Packet Data (CDPD), Global System for Mobile Communication (GSM), and General Packet Radio Services (GPRS), among others. WWANs can span world-wide but are currently limited in data transmission rates, typically from 56Kbps to 300Kbps.

Wireless Local Area Networks (WLAN) include 802.11 (WiFi). WLAN networks utilize unlicensed frequencies and are configured in either *ad hoc* or infrastructure mode. An *ad hoc* WLAN consists of multiple wireless clients communicating as peers to share data without the use of a central Wireless Access Point (WAP). An infrastructure WLAN consists of multiple wireless clients communicating with Wireless Access Point (AP) devices, which are usually connected to a wired network. Devices such as notebook computers or Personal Digital Assistants (PDAs) must generally be within 100 meters of a wireless access point to communicate (100 meters indoors; somewhat longer distances outdoors). New wireless technology is rapidly expanding the useable distances of 802.11 networks to much longer distances. 802.11 networks support fast data communication rates, from 11Mbps to 54Mbps – speeds approaching that of typical wired networks.

Wireless Personal Area Networks (WPAN) such as Bluetooth and InfraRed (IR) are generally designed to allow small devices to communicate over a limited distance. Typical WPANs might be used, for example, to wirelessly interconnect a keyboard or headset to a computer, a computer to a projector, a PDA to a notebook computer, or to communicate among PDAs. Bluetooth supports data transmission rates of up to 720Kbps at distances of up to 30 feet.

Wireless Wide Area Networks (WWAN, non-cellular) High-speed point-to-point wireless connections, sometimes called Fixed Wireless to differentiate them from mobile wireless connections or Wireless LANs. For the purposes of this policy document, WWAN networks are defined as those utilizing FCC licensed radio frequencies (microwave) for point-to-point communication between facilities. This section will not apply to client communication or the use of devices operating within unregulated frequencies. Microwave networks support data communication rates from T1 to OC-3 – speeds are very dependent on the frequency, type of radio and protocol(s) utilized.

Applicability

Agencies within the Executive Department and vendors providing information technology goods and services to these departments must comply with this policy. This policy also applies to entities not part of the Executive Department, and their vendors, including the Constitutional Offices, the Legislature and the Judiciary, that use any wireless networking or services to access the Commonwealth's Wide Area Network (MAGNet). Other entities are encouraged to also adopt this or a similar policy.

Commonwealth's Position

Wireless communications have the potential to increase the efficiency, convenience, and effectiveness of both the delivery of Commonwealth services and access to these services by constituents. The continuing growth in popularity of wireless communications and the proliferation of wireless services, however, pose significant security challenges. Because all wireless networks use electromagnetic waves for data communication, wireless signals may be received by anyone within the transmitting distance of the network access point, whether or not that person is authorized on the network. For this reason, wireless networks pose not only all of the security challenges of a wired network, but also unique challenges that will be new for many state entities.

Entities affected by this policy must first ensure there is a sound business case for the deployment of wireless communications. When wireless communications are implemented, entities must consider this deployment as an extension of their existing fixed-wire network, and mandate use of policy-defined security practices. This will enable the Commonwealth to continue to maintain data and systems confidentiality, integrity, and availability as wireless communication technologies are deployed.

Policy Statement

These policies are intended to address potential security problems with prospective and actual wireless implementations, to offer guidance to ensure the best possible security, and to preclude the use of wireless technology when security cannot be ensured.

- Entities considering the use of wireless communications technologies must document a sound business case that identifies business drivers and total cost of ownership. The total cost of ownership must take into account security standards and best practices that must be implemented as part of the deployment and maintenance of these technologies.
- Entities planning for the deployment of mobile wireless devices and/or wireless networks must follow prescribed standards described in the four Enterprise Wireless Security Standards documents (see Related Documents below).
- Wireless technologies not specifically addressed in this policy or the related Enterprise Wireless Security Standards documents must not be used within the Commonwealth's WAN (MAGNet) or on entity production environments without authorization from the Executive Department Chief Information Officer (CIO)[1] subsequent to a variance recommendation by the Enterprise Security Board.

Roles and Responsibilities

Information Technology Division

- Consult with state entities on the planning and deployment of wireless communications technologies upon receipt of a service request.
- Issue revisions and updates to this policy and related standards, taking into consideration recommendations forwarded by the Enterprise Security Board.
- Approve or deny variance recommendations forwarded by the Enterprise Security Board.

[1] Unless otherwise noted, subsequent references to and use of the term CIO will refer to the Executive Department CIO

Enterprise Security Board

- Recommend revisions and updates to this policy and related standards.
- Review variance requests and forward recommendations to the CIO for approval.

State Entities

- Ensure compliance with this policy for all prospective and actual wireless communications deployments including vendor oversight.
- Ensure all wireless communications deployments in the state entity are sanctioned and supported by the entity's information technology staff in compliance with this policy and related standards.

Vendors

- Ensure that all IT systems and applications developed by or for Executive Department agencies or operating within the Commonwealth's Wide Area Network (MAGNet) conform to this and other applicable Enterprise Information Technology Policies, Standards and Procedures promulgated by the CIO. Non-conforming IT systems cannot be deployed unless the purchasing entity and their contractor have jointly applied for and received in writing from the CIO or designee, notice that a specified deviation will be permitted.

Compliance

All state entities using any wireless technology to access MAGNet must complete an annual compliance survey documenting reasonable assurance that compliance with this policy and its related standards has been achieved. Said documentation may be subject to external review via the Office of the State Auditor, or other parties, authorized to conduct periodic information technology audits to ensure best practices and compliance with enterprise and entity policies.

Related Documents

- Enterprise Wireless Security Standards:
    - Wireless Mobile Communications
    - Wireless Local Area Networks
    - Wireless Personal Area Networks
    - Wireless Wide Area Networks
- Enterprise Information Security Policy
- Enterprise Remote Access Security Policy
- Enterprise Security Variance Policy and Procedures (under development)

Points of Contact

Questions related to this policy should be directed to the Chief Information Security Officer, Enterprise Security Management, within the Information Technology Division.